CYBERSECURITY VIRTUAL LAB AS A SERVICE

Authors: Anti E., Vartiainen T.

Organizations: UVA,

Project: CR-DES

Submission Date: Vaasa June .2023

Vipuvoimaa EU:lta 2014–2020

Contents

BACKGROUND 3
SERVICE DESCRIPTION 4
VALUE PROPOSITION 13
SERVICE ARCHITECTURE 14
SERVICE ECOSYSTEM 15

Figure 1 Governance Structure 5
Figure 2 Service Requirements 6
Figure 3 Integration Plan 12
Figure 4 Service Ecosystem 16

Table 1 Goals 4
Table 2 Service Subscription Strategies 7
Table 3 Categories of Users and Subscription Plans 7
Table 4 Service Testing 9
Table 5 Security Testing 10
Table 6 Testing Plan 10
Table 7 Risk Management Plan 11
Table 8 Value Proposition 14

CYBER SECURITY VIRTUAL LABORATORY OPERATING MODEL

BACKGROUND

Critical infrastructures are the systems and assets required for a society's and economy's operation. These systems include physical infrastructure, such as telecommunications, electric power systems, natural gas and oil, banking and finance, transportation, water supply systems, government services, emergency services, and cyberinfrastructure, such as information technology networks and data centers. People and businesses rely on critical infrastructure daily, and any disruption or damage to these systems can seriously affect public safety and national security. Critical infrastructure systems are frequently the target of physical and cyber attacks by individuals, groups, or state-sponsored actors seeking to disrupt or disable them due to their importance. Various safeguards, such as risk assessments, security protocols, and emergency response plans, are constantly reviewed and implemented to protect these infrastructures.

For example, electric, oil, and gas power systems have undergone many technological transformations. The need to address several issues, such as generation diversification, optimal asset deployment, demand response, energy conservation, and a decrease in the industry's overall carbon impact, has led to the implementation of smart or intelligent grid systems. Smart grids are networks that integrate technology and the actions of all connected users to ensure efficient, sustainable, economic, and secure supplies and distribution. Therefore, smart grids integrate various energy sources such as electricity, gas, and water and optimize their distribution. The infusion of technology means smart grids transmit information through an information infrastructure and are increasingly targeted for cyber attacks.

Continuous research and training to improve cyber security skills are required to prevent complex and innovative ways of attacking critical infrastructure systems. The cyber security virtual laboratories create an avenue to aid research, training, and innovation. This document focuses on developing an operating model for a virtual cybersecurity laboratory. The document is structured as follows:

- SERVICE DESCRIPTION
- VALUE PROPOSITION
- SERVICE ARCHITECTURE
- SERVICE ECOSYSTEM

SERVICE DESCRIPTION

Overview of the Service

To meet today's cyber security training requirements to defend against attacks on critical infrastructure such as smart grids, the need for collaborative research, enabling higher education, and professional development necessitates the creation of a virtual cybersecurity laboratory that includes all operating systems, servers, software, applications, and simulation data. Because of technological advancements and the widespread use of digital devices, cyber security researchers, students, and organizations must keep up with, track, and prevent new and complex techniques from attacking critical infrastructure. These digital evolutions mean there must be more proactive efforts to research, train, and find solutions to cyber-attacks. This section will describe the combination of strategic plans, governance structure, risk management plans, and processes that will be used to create business outcomes, deliver services and create value.

Strategy and Planning

The primary objective of the cyber security virtual laboratory is to provide simulation-based cyber security education and training for students, organizations, and research nationally and internationally. The virtual laboratory's objectives include research projects on energy system cyber security and developing international and national cooperation. The cyber security virtual laboratory will create virtual environments designed for various training and experiments, simulating the practical and theoretical side of cyber-attacks on smart grids.

Strategic Plan

The strategic plan outlines the virtual laboratory's vision, mission, and goals.

Vision

1. Develop and Create solutions-based cyber security services for smart grids nationally and internationally.
2. Build cyber security human capabilities through training and research.

Mission

1. Provide real-time information on current and emerging security threats and vulnerabilities for smart grids.
2. Commercialize the simulation platform into paid service products.
3. Implementation of new R&D projects.

Goals	Description
Real-Time Simulation	Develop Testing and Real-time scenarios on security threats.
Training	Provide Training Services for security professionals.
Research and Development	Provide a Platform for further R&D

Table 1 Goals

Governance Structure

The governance structure will include a review of stakeholder needs, conditions, and options that will aid in developing the cyber security virtual labs objectives. It will also guide goal prioritization, decision-making improvement, and continuous performance monitoring. A steering and technical committee must be included in the structure to manage the virtual laboratory's operations and guide decision-making. The committees will ensure that the cyber security virtual labs plan's application, management, and review are consistent with the defined goals and objectives. Their primary goal is to provide strategic direction, make business and project priorities decisions, and ensure conformity to IT/OT best practices.

The figure below describes the governance structure and its internal operations.

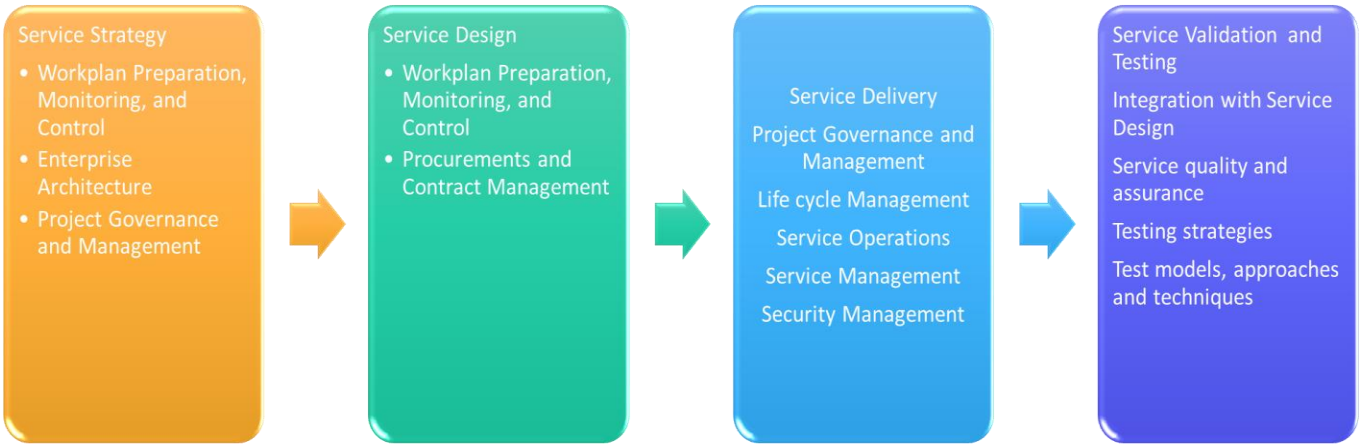

Figure 1 Governance Structure

Service Strategy

The steps for preparing and managing the platform work program will be defined, including objectives, activities, expected results, performance indicators, and related human and financial resources. The work plan must include a high-level, multi-year outlook and a more detailed annual work plan focused on implementing the cyber security platform, simulations, and services. There must be a clear vision for systems, processes, and information and a defined development and improvement plan for the platform's application and infrastructure. A strategy for identifying and integrating new and emerging technologies must be developed.

Service Design

Per the service strategy, the work program will plan and organize resources, such as physical or digital artifacts, developers and customers, workflows, and procedures. A procurement plan must be designed to define the platform's and services' procurement needs and requirements and when and how procurements will be made. A contract management structure will aid in the smooth execution and management of contracts. The service design process will include the following:

Service Requirements

The service requirements of the cyber security platform must include the components required for developing and delivering services. Most importantly, ensure the feasibility of services on the platform. The figure below depicts the components of the service requirements.

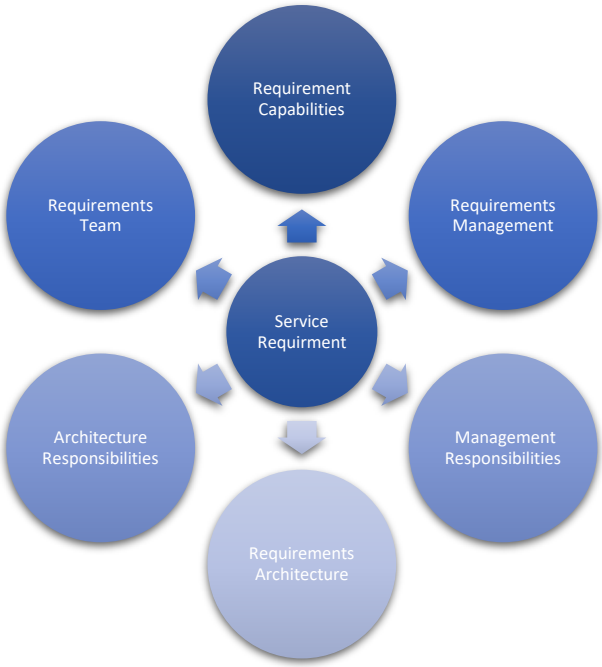

Figure 2 Service Requirements

Requirements Capabilities: Functions to collect functional and non-functional, physical, service offerings, cost, risk management, service delivery, agreements, and service validation requirements.

Requirements Management: This enables and ensures that the management and capabilities of the virtual lab's service requirements are controlled, balanced, and aligned with the mission and needs.

Management Responsibilities: Managing ideas, requirements, plans, risks, opportunities, reviews, decisions, and action items**.**

Requirements Architecture: Provide a management structure to ensure feasibility in terms of functional requirements, physical requirements, non-functional requirements, service requirements, cost requirements, quality requirements, and delivery requirements

Architecture Responsibilities: Providing service architecture concepts, descriptions, models, viewpoints, specifications, and analyses.

Requirements Team: Handles integration, data, configurations, records, information utilization, and system requirements.

Service Offerings

A portfolio of needed service offerings must be created based on the identified service requirements. These service offerings may include :

1. Real-time co-simulation SCALABLE EXataCPS and HYPERSIM OPAL-RT
2. CPS testing scenarios that provide a hands-on demonstration of the impact of MODP Attacks on the cyberspace of energy systems
3. CPS testing scenarios that assess offensive aspects of the cyberspace
4. Cloud-Based Lab.

These services will aid in research and training on threat intelligence, vulnerability assessments, penetration testing, incident response, and security awareness. The service offerings should be scalable and adaptable to changing needs and requirements.

Commercializing the Services Offerings

In line with the overall strategy and goals of the virtual laboratory, the target audience, and the services offered, the following strategies will be adopted in determining free subscriptions and paid services in the table below.

Free Subscription	Paid Services
Level of Access: Limited access to the virtual lab or a specific set of services	Service Tiers: Different tiers of services, such as levels of support, response times, or data processing capabilities
Services Offered: Basic services or a limited set of features of the paid services.	Pricing Model: Charging based on usage, subscription-based pricing, or project-based pricing
Time Limit: A trial period of a few days or weeks or an ongoing subscription with limited access	Marketing and Sales: Digital marketing campaigns, targeted advertising, webinars, or networking with potential clients.
Data Limitations: Limits on the amount of data that can be processed, stored, or analyzed	Customer Support: Support through multiple channels, such as phone, email, and chat(e.g., Chatbots)
Upgrades and Upsells: Upgrade to paid services and what additional features and benefits are available	Scalability: Ensure that the paid services can be scaled as the demand grows

Table 2 Service Subscription Strategies

The table below describes the categories of Users, Clients, or Customers and Subscription plans.

Customers/Clients	Services	Subscription
Students	Cyber Security Exercises	Free Subscription
Researchers	Research and Development	Free/Paid Services
Security Professionals	Training, Simulations	Paid Services
Organizations	Testing, Training, Projects, Simulations	Paid Services

Table 3 Categories of Users and Subscription Plans

Service Agreements

Service agreements with all stakeholders and partners must be developed for the virtual laboratory to ensure service levels are clearly defined and agreed upon. The scope of services, service level objectives, pricing, and terms and conditions should all be outlined in the agreements. To remain relevant and practical, there must be a review and updates of agreements regularly.

Service Delivery

Service delivery processes must be established for the virtual laboratory to ensure services are delivered efficiently and effectively. These processes must include service request management, incident management, security management, change management, and service reporting. The processes should be documented and communicated to ensure stakeholders understand how to interact with the virtual laboratory.

Service request management

1. Requires receiving, categorizing, prioritizing, and resolving service requests.
2. Establishing a service desk or a help desk to receive service requests.
3. Categorize requests based on their type and priority and should be assigned to the appropriate team for resolution.
4. Maintaining a knowledge base of frequently asked questions and known issues to help resolve requests quickly and efficiently.

Incident management

1. Identify, track, and resolve incidents impacting the cyber security lab.
2. Establish an incident response team to investigate and resolve security incidents.
3. The team should have a well-defined process for incident management, including incident detection, assessment, and response.
4. The incident response team should work closely with other IT and research teams to resolve incidents quickly and effectively.

Change management

This process manages IT/OT infrastructure changes and research systems not to impact cybersecurity. Any changes affecting cyber security must be reviewed and approved. Change requests, assessment, approval, and implementation should all be part of the change management process. Testing and validation should be part of the change management process to ensure that changes are implemented correctly and not introduce new vulnerabilities.

Service Validation and Testing

The goal is to ensure that the services associated with the cyber-security platform are of the required quality. This will ensure integration with service design, quality assurance, testing strategies, test models, approaches, and techniques. It will be an iterative service

improvement process that will be used to achieve service quality management. These activities will increase the efficiency of the services and processes on the platform.

Testing methods

Testing is divided into Service testing and Security Testing for critical infrastructure and smart grids. The table below explains the types of tests that can be conducted on the platform.

Service testing will comprise testing and evaluating the software or applications' functionality, performance, usability, and security. The testing methods are explained in the table below.

Test	Purpose
Unit testing	For testing individual methods and functions of the classes, components, or modules used by the virtual lab
Integration tests	Verify that different modules or services used by virtual labs work well together. E.g., testing the interaction with the database or ensuring that microservices work together as expected.
Functional tests	Focus on an application's business requirements in verifying an action's output.
Performance testing	Evaluates how a system performs under a particular workload. These tests help measure the virtual lab's reliability, speed, scalability, and responsiveness.
End-to-end tests	Replicates a user behavior with the software in a complete application environment. It verifies that various user flows work as expected. For example, logging in or more complex scenarios verifying email notifications, online payments, etc.

Table 4 Service Testing

Through our service offerings, security testing grids will simulate how resilient smart grids and critical infrastructure can perform and deal with all potential threats, such as cyber-attacks, Insider threats, and equipment failure.

The testing methods are described as follows:

Methods	Description
Endpoint Detection and Response (EDR)	Testing to simulate insider threats for smart grids to assess businesses' abilities to recognize and respond to malicious acts by trustworthy insiders. This test monitors and defends endpoints against sophisticated threats and attacks on Intelligent Electronic Devices (IEDs), smart metering systems, Substation Automation Systems (SAS), Communication Gateways, and Control Center Systems. EDR tests are designed to identify, investigate, and respond to abnormal endpoint activity in real-time.

Security Information and Event Management (SIEM)	This method will replicate the centralization of security event data collecting, analysis, and correlation from diverse sources within a system or network. In the context of smart grids, SIEM is critical for monitoring and handling security incidents to protect the grid's infrastructure and data's integrity, availability, and confidentiality.
User and Entity Behavior Analytics (UEBA)	This method analyzes the behavior patterns of users and entities within a system or network to detect anomalies, identify potential insider threats, and mitigate security risks. Using UEBA to simulate insider threats in a cyber security virtual laboratory for smart grids can help organizations assess the effectiveness of their UEBA solutions in detecting and responding to insider threats.
Insider Threat Management (ITM)	This method entails the techniques, tools, and strategies businesses use to detect, prevent, and respond to insider threats. Using ITM to simulate insider threats in a cyber security virtual laboratory for smart grids can assist organizations in assessing their ITM capabilities and readiness to cope with such attacks. In the virtual lab, SCADA systems, smart meters, and communication devices can be modeled to see if ITM can mitigate insider threats.

Table 5 Security Testing

Testing Plan

Steps	Description
Determine the Test Scope	Decide on the type, services, and parameters for testing.
Define the Test Cases	Design test cases to cover and identify a wide range of scenarios and potential issues and bugs
Identify Testing Tools	Decide on the testing tool.
Develop Testing Procedures	Decide on the steps, data to be collected, and expected outcomes.
Conduct Testing	Perform the actual tests.
Analyze Results	Identify bugs and issues found, document and prioritize according to the urgent need for a solution.
Address Issues	Fix the issues, make necessary changes, and re-test.

Table 6 Testing Plan

Service Metrics and Reporting

There must be a service reporting mechanism for collecting, analyzing, and presenting data and information related to service performance. The mechanism should include regular reports on service availability, incident response times, customer satisfaction, and other key performance indicators. The reports should be clear and concise and provide actionable insights for improving service performance.

Security Management

Security management will ensure the confidentiality, availability, and integrity of the platform's data, information, and services. This includes developing a risk management plan.

Knowledge Management

Knowledge management captures, stores, and shares cyber security knowledge and information. The virtual laboratory should have a knowledge management system with a knowledge base of frequently asked questions and known issues. The system should also include a mechanism for sharing knowledge and information among team members and with the community of users.

Risk Management Plan

The risk management plan informs teams of the steps to identify, analyze, and respond to all risks that may affect the virtual laboratory's cyber security.

Potential Risks	Severity of Risk	Mitigation Strategies
Unauthorized Access	High	Data Encryption: Data encryption should be implemented on all sensitive data to protect it from unauthorized access
Data Breaches	High	Regular Backups: Regular backups should be performed to ensure that data can be restored in case of data breach.
Software Vulnerabilities	High	Vulnerability Scanning: Regular vulnerability scanning and testing should be performed in the virtual laboratory to identify vulnerabilities in the system
Malware and Ransomware Attacks	High	Use Antivirus and Antimalware Software, Regularly Update Software and Operating Systems, Implement Firewall Protection, and Limit User Access.
Insufficient User Authentication and Authorization	High	Access Controls: Implement a strong access control policy that includes strong passwords, two-factor authentication, and regular password changes
Physical Damage	Low	Implement physical security such as access control, surveillance cameras, and alarms, Regular Maintenance

Table 7 Risk Management Plan

Responsible Team

The incident response team will monitor and resolve incidents quickly and effectively. The incident response team will include key personnel such as the IT manager, security analyst, and legal counsel.

Response Plan

To keep attacks from spreading, the incident response team will identify and contain them. Disconnecting affected systems from the network and deactivating user accounts may be

necessary. In addition, the team will conduct a thorough investigation into the incident to determine the cause, scope, and extent of the breach. The incident must be reported to law enforcement and affected parties, such as users or partners. Finally, once the incident has been contained and investigated, work to restore operations and ensure the security and functionality of all systems.

Following the resolution of the incident, the incident response team should conduct a review to identify any flaws in the response plan and make any necessary updates or improvements to avoid future incidents.

Communication Plan

There must be a well-developed communication plan with message templates, timelines for communication, testing of the plan, and staff training on their roles and responsibilities in communicating with partners and stakeholders. In case of any attacks, the following steps should be followed in communicating with stakeholders and partners:

1. Identifying all stakeholders who need to be informed about the security incident or breach, including users, management, and external partners
2. Inform them about the incident, the potential impact, and actions that need to be taken on their part.
3. Deliver the message to partners and stakeholders via email, phone, social media, or press releases.

Integration plan

The integration strategy specifies the steps and procedures of combining systems or processes into the virtual cybersecurity laboratory. The following steps must be followed:

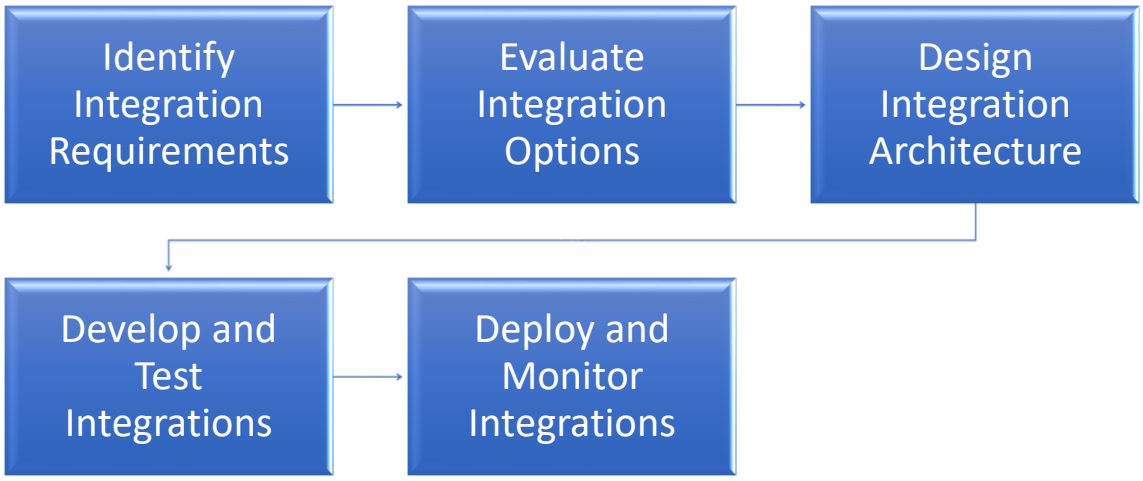

Figure 3 Integration Plan

When evaluating the integration options, it is crucial to determine whether to develop custom integration code, use off-the-shelf integration tools, or leverage cloud-based integration platforms and consider cost, complexity, scalability, and security factors.

VALUE PROPOSITION

Our Cyber Security Virtual Laboratory provides a complete and cutting-edge platform for simulating cyber attacks and testing smart energy grid security. Energy companies and grid managers can use our laboratory to rapidly identify vulnerabilities and potential threats, evaluate the efficacy of their security measures, and implement solutions to improve the resilience of their infrastructure. Researchers, security professionals, and students can use a well-designed platform to perform academic research, studies, and comprehensive training in a secure and controlled environment. Our platform allows users to simulate real-world attacks and assess their effect on energy grid operations and systems by leveraging cutting-edge technologies and methodologies.

Target Group	Value Proposition
Energy Companies and Other Organizations	• Improved cyber resilience as organizations get a comprehensive approach to cyber security, stay ahead of emerging threats and mitigate risks. • Cost-effective testing as users tests their security measures in a safe and controlled environment, avoiding the cost and disruption associated with testing in the live system. • Research and Development collaboration between energy companies, grid operators, and other stakeholders, promoting a shared understanding of cyber security risks and solutions • Training and Support from setup and configuration to ongoing maintenance and training, ensuring that organizations get the most value from their investment in our virtual laboratory
Researchers and Students	• Real-world simulation for researchers and students to test and develop their skills in a safe and controlled environment • Accessibility to explore and experiment with different cyber security scenarios and techniques • Cost-effective as it saves researchers and students costs associated with building and maintaining physical labs • Collaboration to solve complex security challenges, share knowledge, and exchange ideas.
Security Professionals	• Comprehensive training opportunities for security professionals to

	keep their skills and knowledge up to date • Realistic simulation for security professionals to gain practical experience and develop their skills in a safe, controlled environment • Risk-free experimentation for security professionals to experiment and learn without the fear of causing harm or consequences. • Collaboration between security professionals from different locations and organizations • Cost-effective for organizations as they do not have to build and maintain physical labs

Table 8 Value Proposition

SERVICE ARCHITECTURE

The Cyber Security Virtual Laboratory service architecture comprises several components that provide a comprehensive and secure testing environment.

Front-end Interface:

The front-end interface is the entry point for users to access the laboratory. It has a web-based user interface allowing users to register, log in, and select the simulation or testing they want to perform. The interface should be user-friendly, responsive, and accessible from multiple devices and browsers.

Simulation Engine:

The simulation engine is the core component of the laboratory that provides the capability to simulate cyber-attacks. It is designed to replicate various attack scenarios, including insider threats, and to generate realistic test results. The simulation engine should be scalable, reliable, and capable of running multiple simulations simultaneously.

Data Management System:

The data management system is responsible for storing and managing the data generated by the simulation engine. This includes data related to the simulated attacks, system logs, and user data. The data management system should be designed to ensure data privacy and security, with solid encryption and access controls in place.

Reporting and Analysis Module:

The reporting and analysis module provides a dashboard for users to view and analyze the test results generated by the simulation engine. The module should provide real-time data visualization and reporting features, allowing users to monitor the progress of simulations, assess vulnerabilities, and generate reports for stakeholders.

Security Controls:

Security controls are a critical component of the laboratory architecture. They should be implemented throughout the system, including at the user interface, simulation engine, and

data management levels. Security controls should include multi-factor authentication, encryption, access controls, and intrusion detection systems.

Integration with Smart Energy Grids:

The laboratory should be designed to integrate with smart energy grids, allowing energy companies and grid operators to test their security measures in a realistic environment. The integration should ensure that the laboratory does not interfere with the normal grid operation and include firewalls and network segmentation measures.

Maintenance and Support:

Maintenance and support are critical components of the laboratory service architecture. The laboratory should be designed to be scalable, resilient, and easy to maintain, with regular updates and patches to ensure that it remains secure and up-to-date. Support should be provided to users, including training, documentation, and a help desk for technical support and issue resolution.

SERVICE ECOSYSTEM

The broader environment in which the laboratory functions is the service ecosystem. It encompasses all the individuals, processes, and systems interacting with the laboratory and the regulatory and environmental considerations influencing its operations.

Users/Clients: Energy businesses, grid operators, cybersecurity experts, government regulators, researchers, and students are among the participants in the laboratory's service ecosystem. Each of these actors is responsible for guaranteeing the smart energy grid's security and resilience, and they interact with the laboratory in different ways. The laboratory is used by energy businesses and grid operators to evaluate their security measures, while cybersecurity professionals provide assistance and experience in detecting and resolving vulnerabilities. Government regulators may need the usage of the laboratory to ensure compliance with cybersecurity legislation, and other stakeholders may be concerned about the grid's security and resilience.

Processes: The laboratory's service ecosystem encompasses the many procedures for testing and evaluating the smart energy grid's security. These include finding vulnerabilities, simulating cyber-attacks, assessing test results, and implementing risk-mitigation strategies. The laboratory provides a controlled environment for these procedures, allowing energy businesses and grid operators to safely and securely test their security measures.

Systems: The service ecosystem comprises the many technologies and infrastructures supporting the laboratory's functioning. The systems contain the simulation engine, data management system, reporting and analysis module, security controls, and other laboratory components. These solutions are designed to work in tandem to give energy firms and grid operators a comprehensive and secure testing environment.

Regulatory and Environmental Factors: The legislative and environmental aspects of the laboratory's service ecosystem include the numerous rules, regulations, and standards that regulate the operation of the smart energy grid. These include, among other things,

cybersecurity restrictions, privacy legislation, and environmental regulations. The laboratory must follow these regulations to guarantee that its operations do not break any laws or regulations. Furthermore, the laboratory must operate in an environmentally efficient manner, limiting its environmental impact**.** The figure below highlights the service ecosystem.

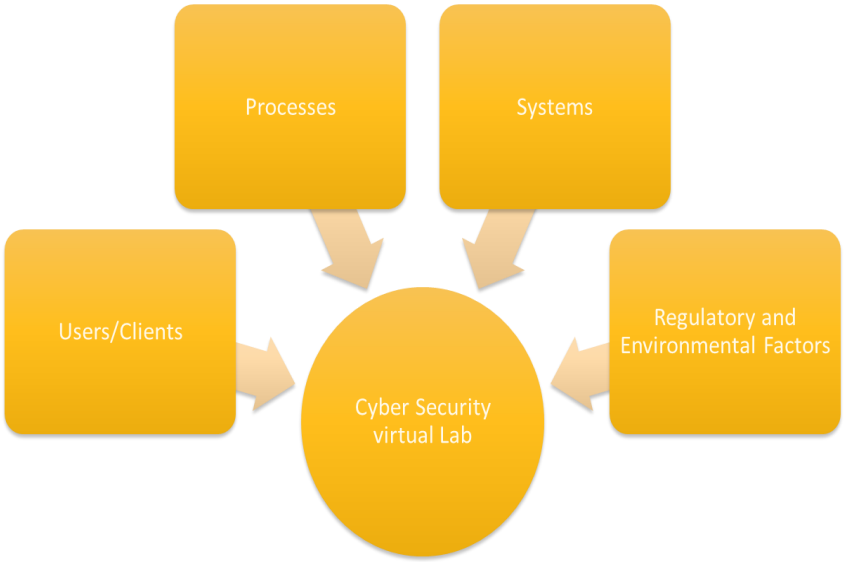

Figure 4 Service Ecosystem

References

Cybersecurity, C. I. (2018). Framework for improving critical infrastructure cybersecurity. *URL: Https://Nvlpubs. Nist. Gov/Nistpubs/CSWP/NIST. CSWP*, *4162018*.

Director Consultation Groups – Core Business IT Target Operating Model 2023—2027. (n.d.).

Gopstein, A., Nguyen, C., O'Fallon, C., Hastings, N., Wollman, D., & others. (2021). *NIST framework and roadmap for smart grid interoperability standards, release 4.0*. Department of Commerce. National Institute of Standards and Technology

Hassan, F. (2010). The path of the smart grid. *IEEE Power and Energy Magazine*, *8*(1), 18–28.

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, *21*(6), 11–25.

Tuballa, M. L., & Abundo, M. L. (2016). A review of the development of Smart Grid technologies. *Renewable and Sustainable Energy Reviews*, *59*, 710–725. https://doi.org/10.1016/j.rser.2016.01.011

Tuunainen, V. K., & Tuunanen, T. (2011). IISIn-A model for analyzing ICT Intensive Service Innovations in n-sided Markets. *2011 44th Hawaii International Conference on System Sciences*, 1–10.

Tuunanen, T., Bask, A., & Merisalo-Rantanen, H. (2012). Typology for modular service design: Review of literature. *International Journal of Service Science, Management, Engineering, and Technology (IJSSMET)*, *3*(3), 99–112.

Tuunanen, T., Myers, M. D., & Cassab, H. (2010). A conceptual framework for consumer information systems development. *Pacific Asia Journal of the Association for Information Systems*, *2*(1), 5.

Williams, K., Chatterjee, S., & Rossi, M. (2008). Design of emerging digital services: A taxonomy. *European Journal of Information Systems*, *17*(5), 505–517.